当資料は、2020 年 12 月 3 日に米国で発表されたプレスリリースの抄訳版です。
米国リリース原文：Dell Technologies Intrinsic Security Helps Businesses Build Cyber Resilience | Dell Technologies US

2020 年 12 月 11 日
デル・テクノロジーズ株式会社

デル・テクノロジーズ、サイバー攻撃に対する企業のレジリエンス（回復力）を確立するためのセキュリティー ソリューションとサービスを発表

すべての製品や機能にセキュリティーを内在させるビジョン「Intrinsic Security」により、サプライチェーン、サービス、インフラストラクチャーを網羅する新たなソリューションとサービスを展開し、先進のセキュリティーを実現

ニュースの概要

- 新しいサプライチェーン セキュリティー ソリューションを発表 – 業界で最もセキュアな法人向け PC[*1] のセキュリティーをさらに強化
- サプライチェーンの完全性の検証、ブート プロセスの保護、動的なシステム ロックダウンをはじめとする独自機能を提供 – サイバー攻撃に対するレジリエンス（回復力）を備えたサーバー アーキテクチャーを強化
- データ セキュリティーにフォーカスしたサービスをインフラストラクチャー ポートフォリオ全体およびサードパーティー製品にまで拡張

2020 年 12 月 3 日、テキサス州ラウンドロック発：
デル・テクノロジーズは、すべての製品や機能にセキュリティーを内在させて、お客様のデータを保護する「Intrinsic Security（イントリンシック セキュリティー）」のビジョンを前面に押し出した新しいソリューションとサービスを発表しました。サプライチェーン、サービス、インフラストラクチャー、デバイスのすべてにセキュリティーを組み込むことで、お客様のリスク軽減とサイバー環境におけるレジリエンス（回復力）の強化をサポートします。

セキュリティー リスクが高まる中、企業は自社および顧客を保護するプレッシャーに直面しています。デル・テクノロジーズが発表した「Dell Technologies 2020 Digital Transformation Index」から、デジタル トランスフォーメーション（DX）にとって最大の障壁は、データ プライバシーとサイバー セキュリティーに対する不安であることが明らかになっています[*2]。また、Futurum Research 社が行った調査によると、外部からのサイバー攻撃に遭った企業の 56%が、その原因をハードウェアまたはシリコン レベルのセキュリティーの脆弱性にあると考えています[*3]。

デル・テクノロジーズの CTO（最高技術責任者）、ジョン ローズ（John Roese）は、次のように述べています。「デジタルによる価値が生み出されると、これに付随するセキュリティーの脅威が発生します。セキュリティーは、デル・テクノロジーズが行うあらゆる物事の基盤になるものです。当社が掲げる Intrinsic Security によるアプローチは、攻撃をかわすとともに、ビジネス リスクの軽減を支援する信頼のテクノロジーとパートナーに対するお客様のニーズに応えます」。

デル・テクノロジーズは、長年にわたり数百人のセキュリティーのプロフェッショナル エンジニアを社内全体に配してセキュリティーをデザインし、サプライチェーン、サービス、インフラストラクチャー、デバイスに組み込んできました。「Dell EMC PowerEdge」サーバーのハードウェア ルートオブトラストおよびデルの PC のオペレーティング システム以下のすべてのセキュリティーから、「Dell EMC PowerMax」のエンド ツー エンドの暗号化および「Dell EMC PowerProtect」のサイバー リカバリー ソリューションまで、デル・テクノロジーズにとってセキュリティーは最優先事項です。

Moor Insights & Strategy 社のプレジデント兼プリンシパル アナリスト、パトリック ムーアヘッド（Patrick Moorhead）氏は次のように述べています。「あらゆる新しいテクノロジーとサービスの中核には、セキュリティーが不可欠です。IT インフラストラクチャーでは、すべての接点にセキュリティーが組み込まれていることは当然として、そのセキュリティーも事後対応的なものではなく、予測的かつ自己防衛的で、全般的なレジリエントを備えていることが必要です」。

エンド ツー エンドの保護によりサプライチェーンとデバイスのライフサイクルのセキュリティーを確保

Futurum Research 社が行った調査では、偽造コンポーネントやマルウェア、ファームウェアの改ざんなど、セキュリティーの脅威に対応するためのベンダー選定において、75%以上の企業がサプライチェーンのセキュリティーを重視すると回答しています[*3]。デル・テクノロジーズは、インフラストラクチャーおよび法人向け PC を対象にした新しいサプライチェーン セキュリティー ソリューションおよびデータ セキュリティーにフォーカスしたサービスによって、このようなセキュリティーの不安を解消します。これらの新しいソリューションは、包括的でセキュアなサプライチェーン プラクティス全体を強化します。

輸送中も PC を保護：デルの法人向け PC は、すでに業界で最もセキュアですが[*1]、さらに複数のサプライチェーン セキュリティー レイヤーと整合性コントロールによって、強化されています。デル・テクノロジーズは、「Dell Secure Development Lifecycle」および標準

のサプライチェーン セキュリティー対策を基盤に、「Dell Technologies SafeSupply Chain」ソリューションを提供します。これらの新しいソリューションの内容は、次のとおりです。

- 「SafeSupply Chain Tamper Evident Services」は、輸送中の PC を改ざんから保護します。工場出荷前、デバイスおよび梱包には、改ざん防止シールが施されます。オプションで、パレットにもシールを施して、さらにセキュリティーを高めることができます。
- 「SafeSupply Chain Data Sanitization Services」は、デバイスのハードドライブへのスパイウェアや不正エージェントの侵入を防ぎます。NIST（米国立標準技術研究所）基準に準拠したハードドライブのデータ消去によって、お客様はデバイスが完全に白紙の状態で自社の企業イメージを加えることができます。

納入時にサーバーの完全性を検証：「Dell EMC PowerEdge」サーバー ポートフォリオでは、サーバーがオーダーから生産を経て、改ざんや不正アクセスされずに納入されていることをお客様が検証するための埋め込み証明書「Secured Component Verification」が、提供されます。デル・テクノロジーズは、ポートフォリオ全体を通じてハードウェアの完全性を暗号により検証するソリューションを提供する初の[*4] サーバー プロバイダーです。 また、「PowerEdge」サーバーは、シリコン ベースのルートオブトラストを含むサイバー レジリエント アーキテクチャーで構築されています。新しい「Secured Component Verification」の内容は、次のとおりです。

- 工場でサーバーが梱包され出荷された後に、システム コンポーネントにいかなる変更も加えられていないことを検証（メモリーやハードドライブのスワップ、I/O の変更など）
- 金融や医療など、厳格に規制の遵守が求められる業種のサプライチェーン セキュリティーの基準を満たすことで、サイバーセキュリティーのリスクから製品を保護
- 複数のサーバーの効率的な検証とデプロイメントをサポート

セキュリティーを確保した状態で資産を再デプロイ、リタイヤ、管理：デル・テクノロジーズは、データ セキュリティーにフォーカスしたサービスの範囲をインフラストラクチャー ポートフォリオ全体に広げました。

- 「Dell EMC Data Sanitization for Enterprise[*5]」および「Dell EMC Data Destruction for Enterprise」のサービスは、対象がデル・テクノロジーズのインフラストラクチャー ポートフォリオ全体およびサードパーティー製品にまで広げられました[*6]。業界およびコンプライアンスの最新標準にしたがって、資産の再デプロイやリタイヤを行うため、デル・テクノロジーズはこれらのサービスをお客様のサイトで提供します。

- 「ハードディスク返却不要サービス エンタープライズ向け（Dell EMC Keep Your Hard Drive for Enterprise）」および「コンポーネント返却不要サービス エンタープライズ向け（Dell EMC Keep Your Component for Enterprise）」[*7]は、デル・テクノロジーズのインフラストラクチャー ポートフォリオ全体を通じて利用できます。コンポーネントを交換した場合でも機密性が求められるデータは常にお客様がコントロールできるので、データ プライバシーの厳格な規制も確実に遵守できます。

カスタマイズ、オートメーション、インテリジェンスでインフラストラクチャーのセキュリティーを確保

Futurum Research 社が行った調査によると、過去 12 カ月間にハードウェア レベルの攻撃または BIOS への攻撃を最低でも 1 回は受けたという企業は 44%に上り、16%はこのような攻撃を複数回受けていることが分かっています[*3]。一定のタイプの脆弱性および悪意ある攻撃から保護するためには、ハードウェアおよびファームウェアのレベルでインフラストラクチャーのセキュリティーを確保する必要があります。デル・テクノロジーズは、「Dell EMC PowerEdge」サーバー ポートフォリオについて、新たなレベルのセキュリティーのカスタマイズ、オートメーション、インテリジェンスによってこれらの課題に応えます。

サーバーのブート セキュリティーをカスタマイズ：あらゆるデバイスにとって、ブート プロセスはセキュリティーの基盤です。ブート プロセスのセキュリティーが突破されてしまうと、攻撃者はセキュリティー コントロールを破り、システムのどこにでもアクセスできるようになってしまいます。お客様の IT スタッフは、デル・テクノロジーズのサーバー セキュリティー機能を活用してサーバーのブートプロセスをカスタマイズし、攻撃対象領域（アタック サーフェス）を減らし、ブートに関係する攻撃を阻止することができます。このデル・テクノロジーズの独自機能[*8]「PowerEdge UEFI セキュアブートカスタマイゼーション」により、業界全体にわたるブートローダーの脆弱性を大幅に軽減することが可能になります。このアプローチは、米国家安全保障局（NSA）が発表した報告書でも検証されています。

サーバーのロックダウンで脅威から保護：「Dell EMC PowerEdge」サーバーの「iDRAC（統合リモート アクセス管理）」が、サーバーおよびリモートの両方でサーバーの自動管理を実現します。お客様は、リブートすることなくシステム ロックダウンの有効化／無効化を切り替えられます。デル・テクノロジーズだけが提供するこの機能が[*4]、サーバーのファームウェアや重要な構成設定データを不注意による変更や悪意ある変更から保護します。最新リリースの「iDRAC9」では、ロックダウン機能がネットワーク インターフェイス コントローラーにまで拡張されており、ロックダウンに対するこれまで以上のコントロール能力

を提供します。最新リリースのその他の特長は以下のとおりです。

- マルチファクター認証（多要素認証）を通じた、これまで以上に強力なセキュリティー コントロール
- 「Dell EMC OpenManage Ansible Modules」による、ユーザー権限の設定やデータ ストレージの暗号化といった「Dell EMC PowerEdge」の重要なセキュリティー ワークフローの自動化
- Redfish API を使用した「iDRAC」の証明書管理による、スクリプトベースの容易なアクセスや全サーバーに対するセキュア消去の自動化

提供について

- 「Dell SafeSupply Chain」は、現在米国の法人向け PC で利用できます。日本国内での販売については未定です。
- 「Dell Technologies Secured Component Verification on PowerEdge Servers」は、2020 年（暦年）末までに提供開始の予定です。
- 「Dell EMC Data Sanitization for Enterprise」および「Data Destruction for Enterprise」のサービスは、すでに提供を開始しています。
- 「ハードディスク返却不要サービス エンタープライズ向け（Dell EMC Keep Your Hard Drive for Enterprise）」および「コンポーネント返却不要サービス エンタープライズ向け（Keep Your Component for Enterprise）」は、すでに提供を開始しています。
- 「Dell Technologies PowerEdge UEFI セキュアブートカスタマイゼーション」は、すでに提供を開始しています。
- 「iDRAC」のセキュリティー アップデートは、2020 年末までに提供開始の予定です。
- 「Dell EMC OpenManage Ansible Modules」のアップデートは、2021 年 1 月 31 日に提供開始の予定です。

*1 デル・テクノロジーズ社内分析に基づく（2020 年 1 月）

*2 「Dell Technologies 2020 Digital Transformation Index」

*3 Futurum Research 社「Four Keys to Navigating the Hardware Security Journey」（2020 年 10 月）

*4 公開データによるデル・テクノロジーズ社内分析に基づく（2020 年 10 月）。「PowerEdge 14G」および「15G」で提供中。「XE7100」「XE7420」「XE7220」「C6420」「C6525」でも提供する予定です。

*5 詳細は、Dell Media SanitizationStatement を参照。 デル・テクノロジーズは、お客様のセキュリティー ニーズや、あるデータ削除方法の別の方法に対する有効性に関する表明については推奨していません。 デル・テクノロジーズが回収したハードドライブに含まれる機密情報または機密情報を保護するのは、お客様の責任です。

*6 デル・テクノロジーズ以外のブランドの製品の適格性は、ベンダーではなくテクノロジーの種類に基づいています。

*7 ハードドライブの保持は、Venue 11 Pro を除き、Chromebook または Venue タブレットでは利用できません。

*8「PowerEdge 14 G」以降から利用できます。顧客証明（Customer Certificate）が必要です。

# # #

■デル・テクノロジーズについて

デル・テクノロジーズ（NYSE：DELL）は、企業や人々がデジタルの未来を築き、仕事や生活の仕方を変革することを支援します。同社は、データ時代に向けて、業界で最も包括的かつ革新的なテクノロジーとサービスのポートフォリオをお客様に提供しています。

# # #

本件に関するお問い合わせ先：
デル・テクノロジーズ株式会社 マーケティング統括本部 広報部
JPCorporateCommunications@Dell.com

共同 PR 株式会社
古川、白武、児玉 Tel: 03-3571-5176 E-mail: delltechnologies-pr@kyodo-pr.co.jp